Biomanager

Version 2.5
11/10/2011

User Manual

Table of Contents

About

Biomanager is suport utility for fingerprint readers.

Functions:

- Readers configuration
- User management
- Finger templates storage
- Upload templates to readers
- Readers firmware update

Software

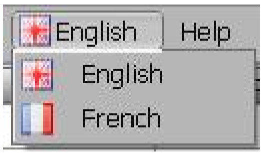
How to start

First time after the installation of Biomanager it is recommended to follow bellow steps in described order:

- Run Biomanager, default password is "admin"
- Select language
- Change Biomanager password
- Set Keycode length if readers with keypad are used
- Add portals
- Add readers
- Add users
- Enroll users fingerprints
- Upload users to readers

Language

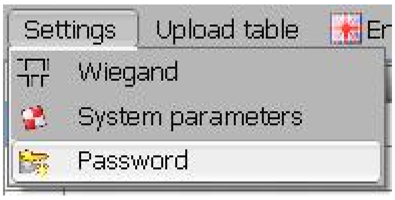
- From main menu select language menu and choose **language**.



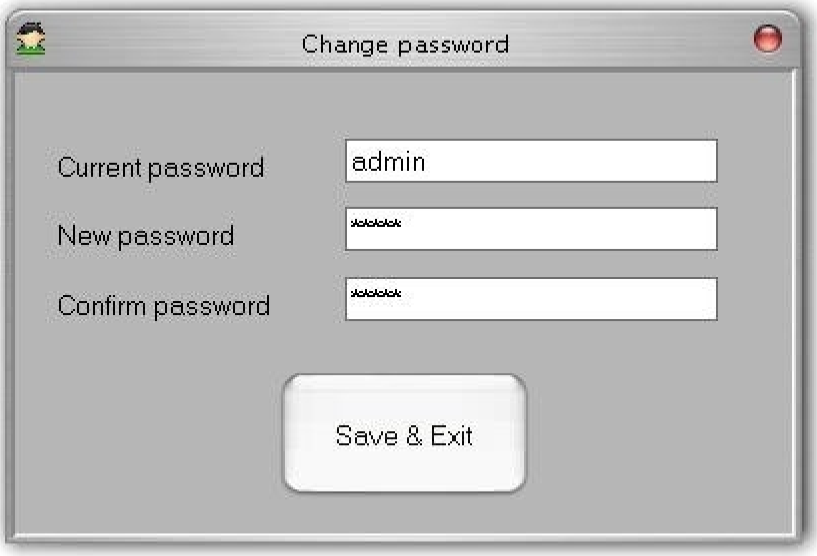
- Restart Biomanager

Password

- From the main manu select **Password** from Settings menu



- Fill password form with current and new password and click on **Save & Exit** button



Current password: admin

New password: *****

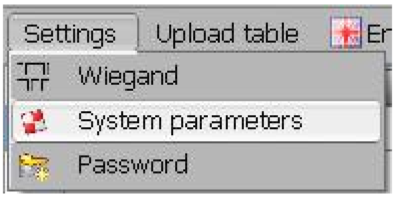
Confirm password: *****

Keycode

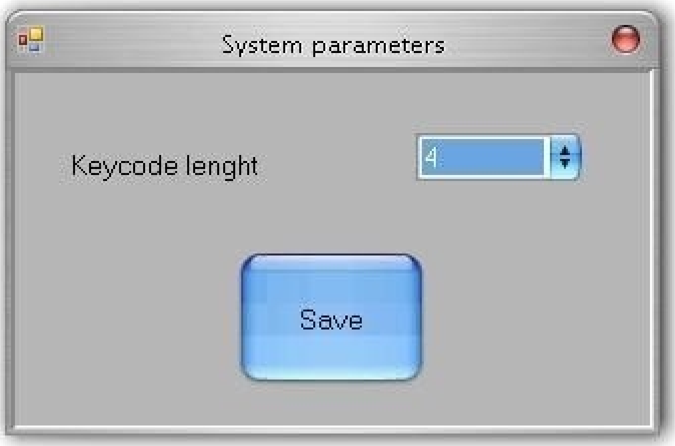
Keycode length is number of digits to be typed at reader to grant access.
Keycode length can be from 1 to 8 digits.
Default length is 4 digits.

Changing Keycode length:

- ○ Select **System parameters** from **System** menu



- ○ From drop-down list select desired value and click **Save** button

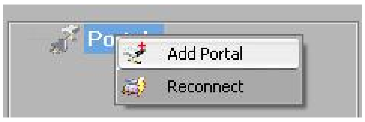


Keycode lenght: 4

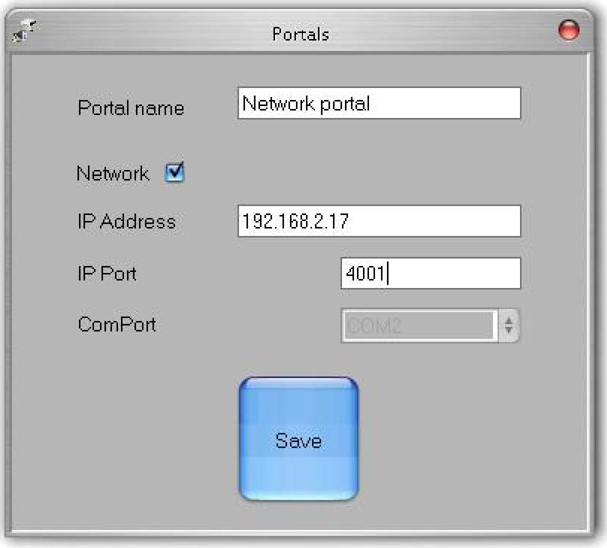
Portals

Add Portal

- Right click on Portals and select **Add portal**



- Fill Portals form
  - Enter portal name by your choice
  - If connection is via network with CNV300 check "Network" box, enter IP address of CNV300, enter IP Port of CNV300
  - if connection is with CNV100 or CNV200 leave check box unchecked and chose serial port from drop-down list


Portals

Portal name: Network portal

Network ☑

IP Address: 192.168.2.17

IP Port: 4001

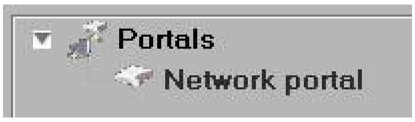
ComPort: COM2

- Click **Save** button

Under "Portalstree appears new portal, with icon

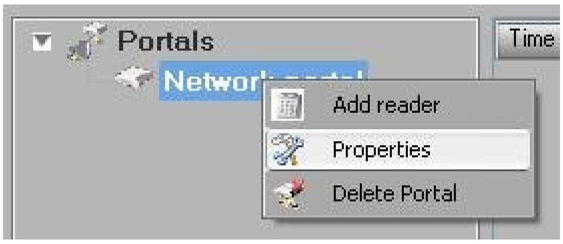
for network and icon

for serial interface

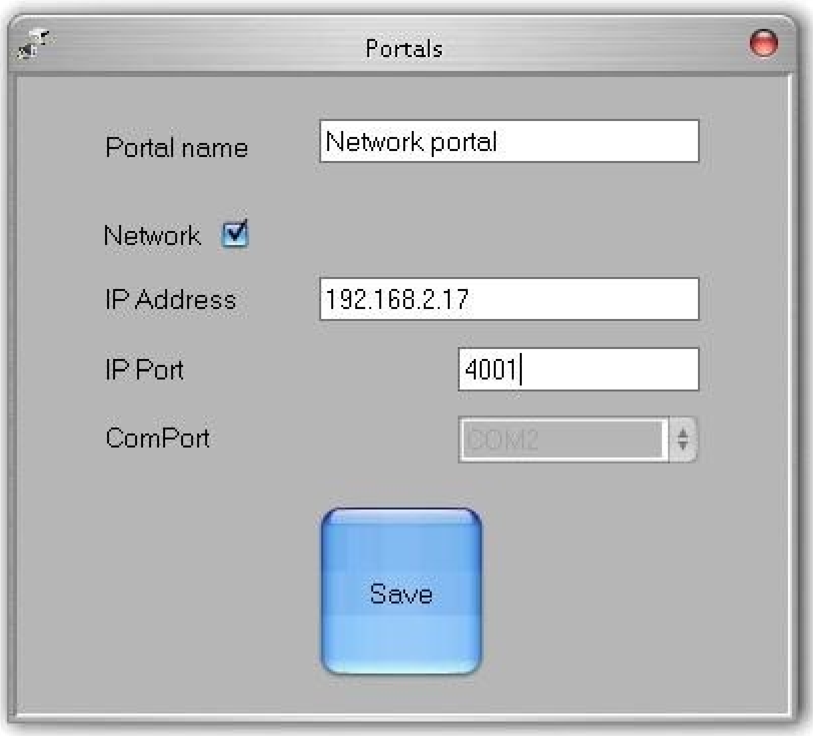


Edit Portal

- Right-click on desired portal and select **Properties**



- ○ Edit values on Portals form



Portal name: Network portal

Network ☑

IP Address: 192.168.2.17

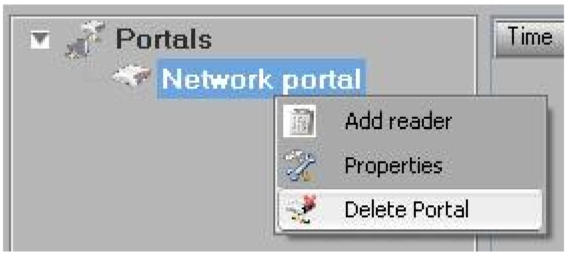
IP Port: 4001

ComPort: COM2

- ○ Click **Save** button

Delete Portal

- ○ Right-click on desired portal and select **Delete portal**



Readers

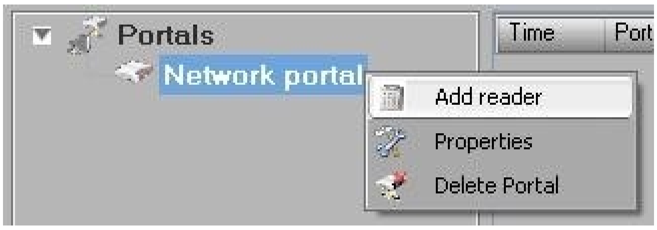
Readers properties

Reader properties may vary depends on type

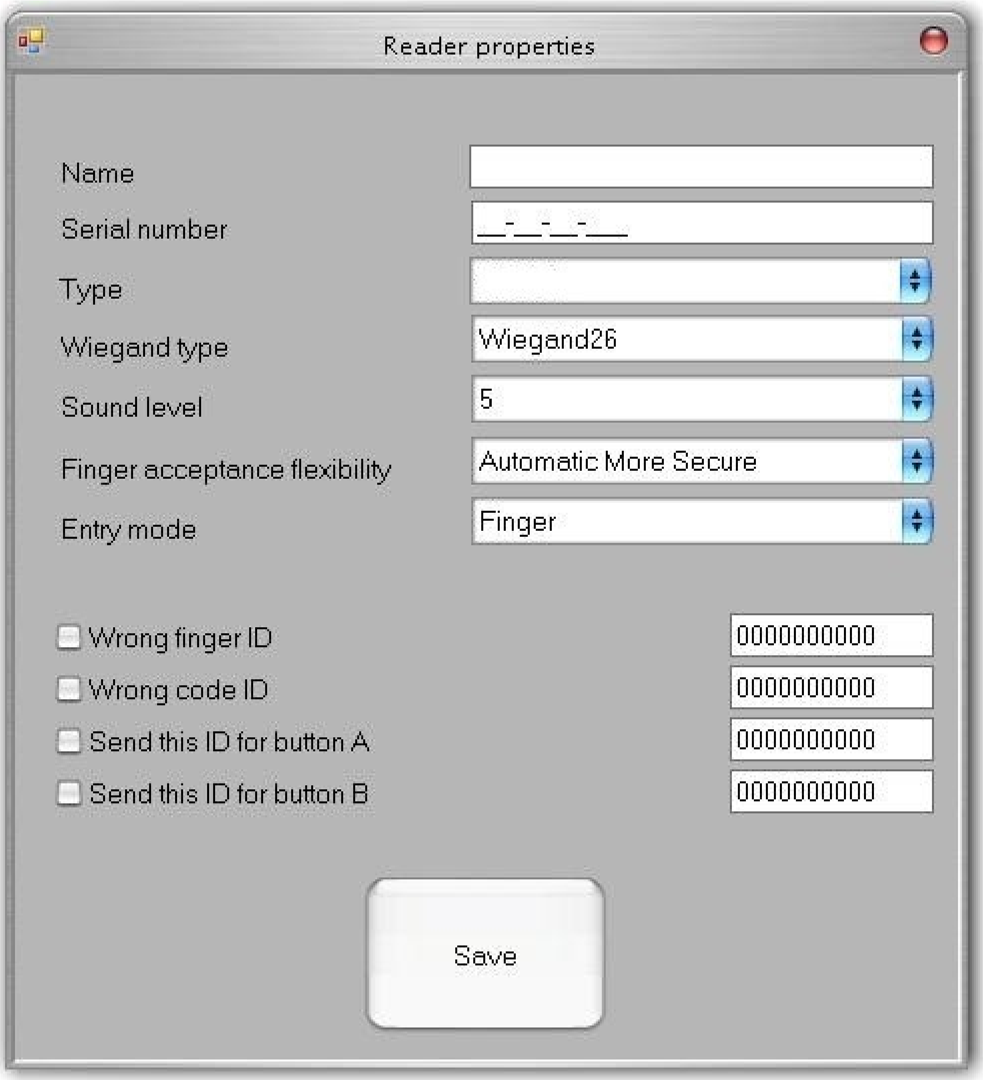
Property	Description	BioXr	BioC BioIn Prox
Serial number	Unique serial number of device, built in by manufacturer	○	○
Wiegand type	Wiegand format sent to reader controller	○	○
Sound level	Level of the sound generated from the reader, 0 = no sound, 9 = maximum volume	○	○
Finger acceptance flexibility	Adjust fingerprint tolerance, recommended default is "Automatic More Secure"	○	○
Sensitivity	Bio-sensor sensitivity, recommended value is 7, most sensitive.	○	○
Entry mode	Reader authorisation mode - Finger, Finger and Keycode, Finger or Keycode	○	
Wrong finger ID	Wiegand code sent if reader do not find finger match, not functional if Finger Entry mode selected	○	
Wrong Keycode ID	Wiegand code sent if reader do not find keycode match, not functional if Finger Entry mode selected	○	
Button A ID	Wiegand code sent if button A is pressed, not functional if Finger Entry mode selected	○	
Button B ID	Wiegand code sent if button B is pressed, not functional if Finger Entry mode selected	○	

Add Reader

○ Right-click on portal connected to reader and select **Add reader**



○ Fill Reader form

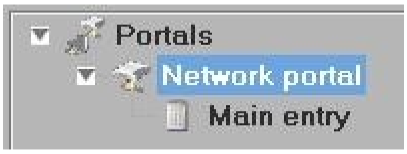


Reader properties

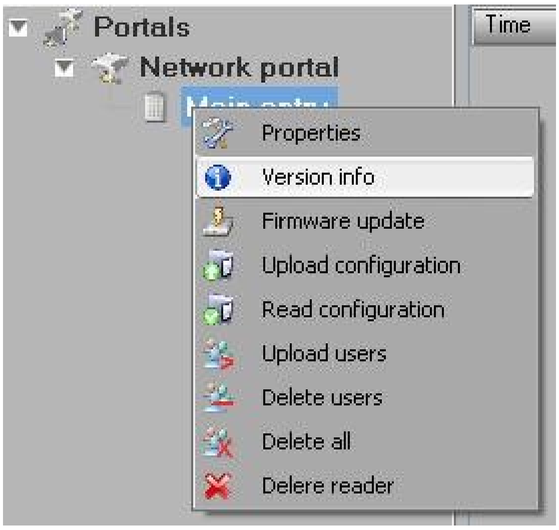
Name	
Serial number	__-__-__-___
Type	
Wiegand type	Wiegand26
Sound level	5
Finger acceptance flexibility	Automatic More Secure
Entry mode	Finger

□ Wrong finger ID	0000000000
□ Wrong code ID	0000000000
□ Send this ID for button A	0000000000
□ Send this ID for button B	0000000000

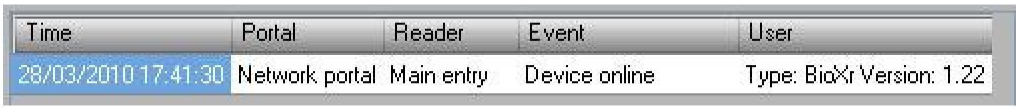
○ Click on **Save** button and reader icon appears under the selected portal



○ Right-click on reader and select **Version info**

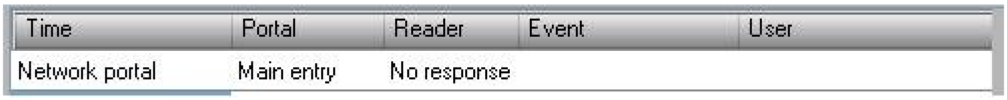


If reader is online, new line is added on top of the event table



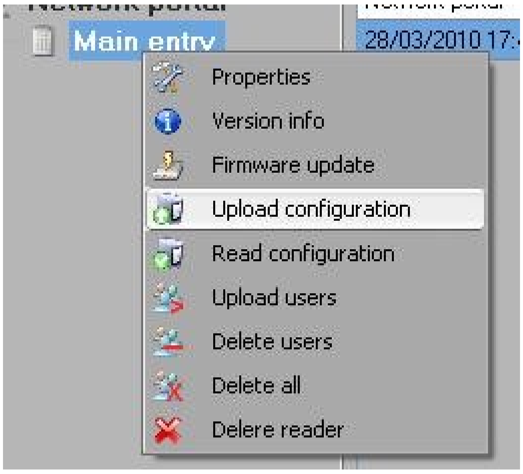
Time	Portal	Reader	Event	User
28/03/2010 17:41:30	Network portal	Main entry	Device online	Type: BioXr Version: 1.22

If reader is not online, following line is added on top of the event table

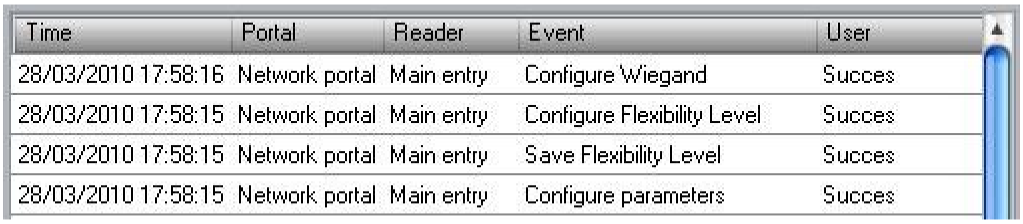


Time	Portal	Reader	Event	User
Network portal	Main entry	No response		

- If reader is online, right click on reader and select **Upload configuration**



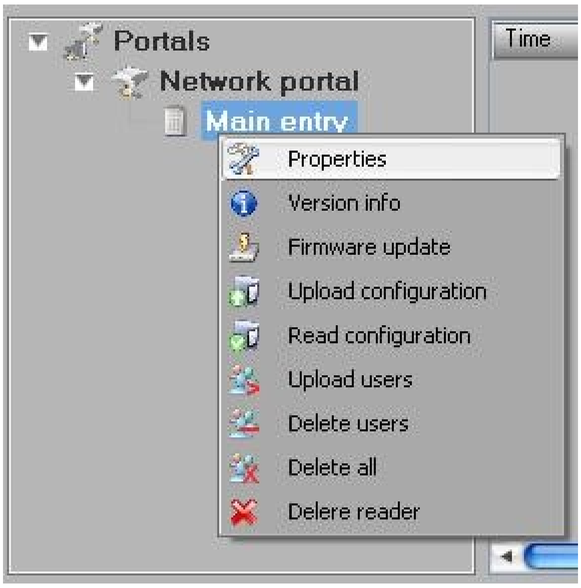
- Check at event table if configuration was successful



Time	Portal	Reader	Event	User
28/03/2010 17:58:16	Network portal	Main entry	Configure Wiegand	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Save Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure parameters	Succes

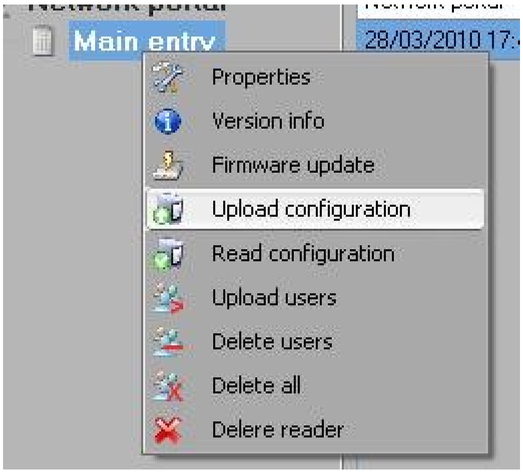
Edit Reader

- Right-click on reader and select **Properties**

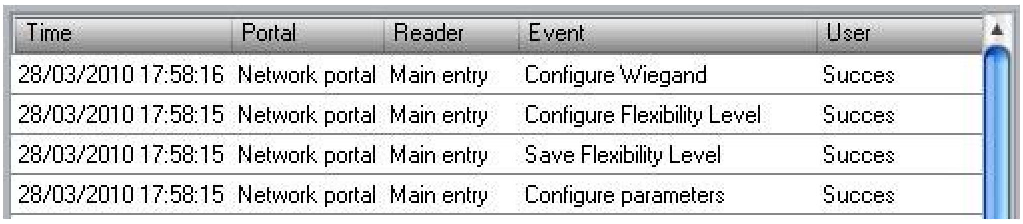


- Edit reader properties and click **Save** button

- Right click on reader and select **Upload configuration**



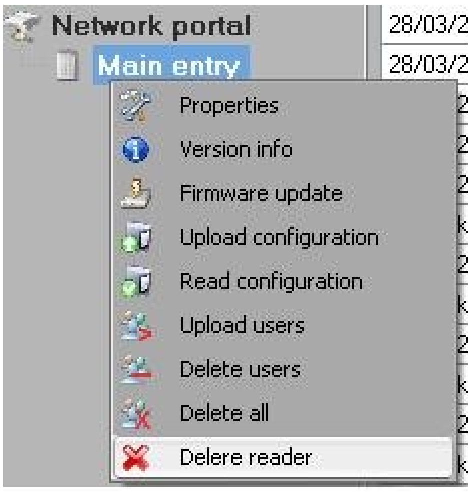
- Check at event table if configuration was successful



Time	Portal	Reader	Event	User
28/03/2010 17:58:16	Network portal	Main entry	Configure Wiegand	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Save Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure parameters	Succes

Delete Reader

- Right-click on reader and select **Delete reader**



Calibrate sensor

- Right-click on reader and select **Calibrate**

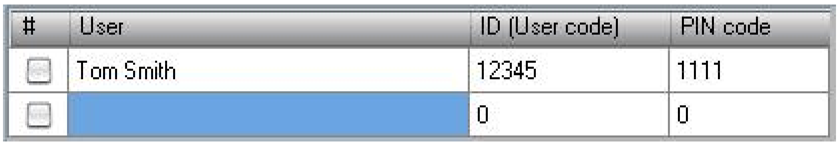
- See events panel to check Calibration flow

It is recommended to do sensor calibration once after reader is mounted. Clean the fingerprint sensor before calibration.

Users

Add user

- At user table, click on last empty user field and enter user name



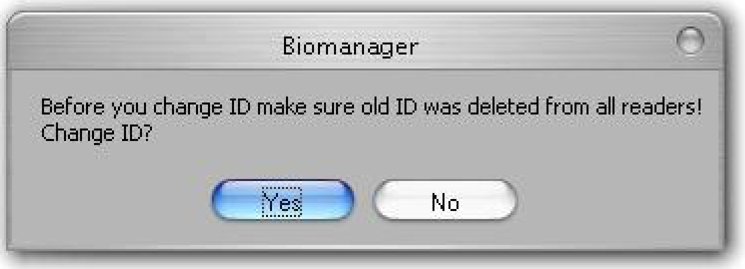
#	User	ID (User code)	PIN code
□	Tom Smith	12345	1111
□		0	0

- Click on ID (User code) field and enter ID number. This number will be send by reader to access controller when user finger is recognised by reader
- Click on PIN code field and enter PIN. PIN code is used at readers with keypad. When PIN code is typed at reader, User ID will be sent to access controller

Edit user

- Find user at user table to edit
- Click on user field for edit (Name, ID or PIN)
- Type new value
- Press Enter on keyboard

Important:
When ID is changed, warning message is displayed reminding that if ID exist in some reader, should be deleted from reader prior to change.

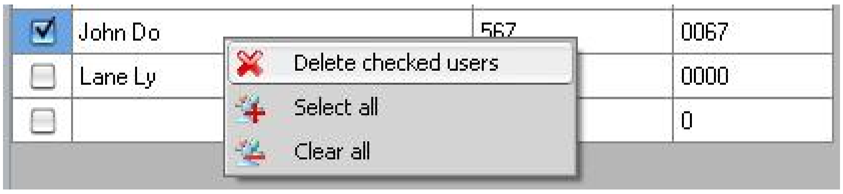


Biomanager

Before you change ID make sure old ID was deleted from all readers!
Change ID?

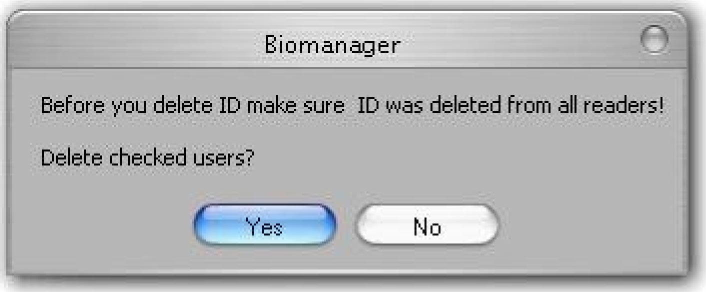
Delete users

- Check users to be deleted
- Right-click on users table
- Click on **Delete checked users menu**



☑	John Do	567	0067
□	Lane Ly		0000
□			0

- Confirm warning message



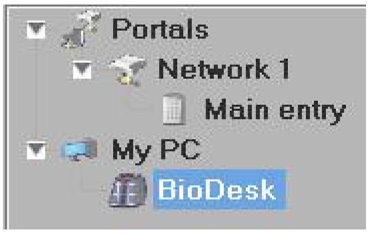
Biomanager

Before you delete ID make sure ID was deleted from all readers!

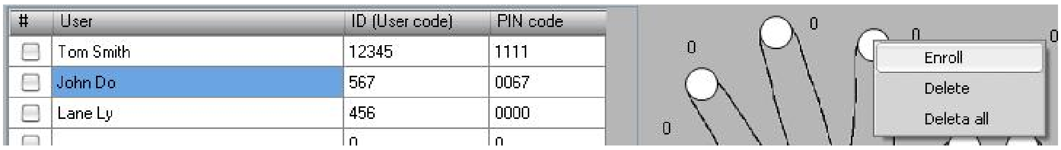
Delete checked users?

Enroll fingers

- Select the User in the User Column, not the check box (the check box is for sending the fingerprints) and the User name cell will turn blue
- Select the Fingerprint reader or Desktop reader BioE from where the enrollment will be done

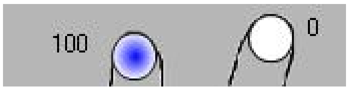


- Right click on the fingertip and select **Enroll**



#	User	ID (User code)	PIN code
□	Tom Smith	12345	1111
□	John Do	567	0067
□	Lane Ly	456	0000
□		0	0

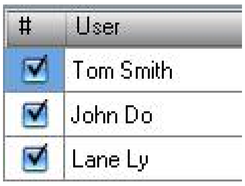
- Swipe the finger on the Reader and the finger tip will become blue, with percentage of successful enrollment given right beside the fingertip



Note: If more fingerprints are added for one user, all the fingers will send the same Wiegand Code to the controller.

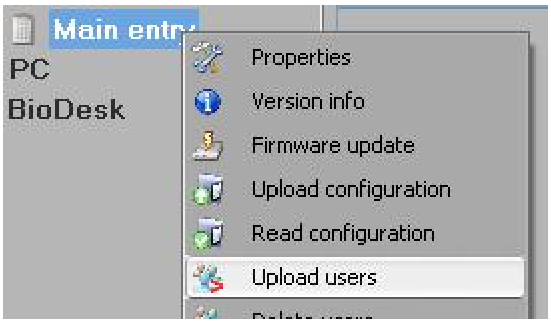
Upload fingerprint to readers

- Check the users which fingers will be sent to the Reader



#	User
☑	Tom Smith
☑	John Do
☑	Lane Ly

- Right-click on the Fingerprint reader those users should be sent and select **Upload users**



- As each user is being sent, the checkbox will become unchecked indicating that the user is successfully sent. In the same time the Amber LED of the Fingerprint Reader blinks

Note: Average time for transferring one finger template is 0,8 sec.
Note: The PIN Codes are also being sent, if there are any.

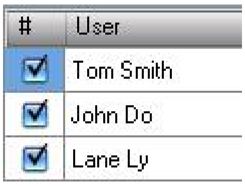
Delete fingerprints

After transferring, the fingerprint are stored in the Fingerprint reader and in the PC.

Deleting can be done only in the software, only in the readers or from the both places.

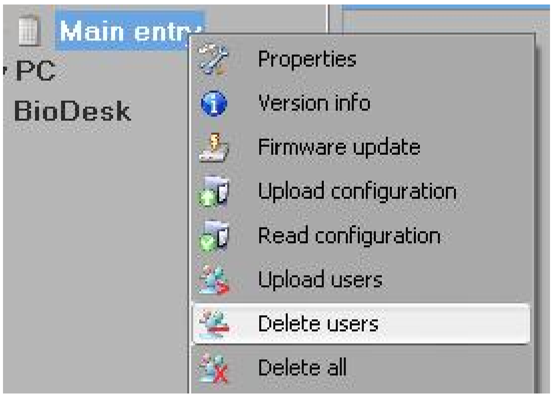
Deleting one user from the fingerprint Reader

- Select the users checkbox.



#	User
☑	Tom Smith
☑	John Do
☑	Lane Ly

- Right click on the Reader and select **Delete Users**



- The user is deleted from the reader, but his fingerprints are still in the software's database. They can be sent ones again without the need of re enrollment.

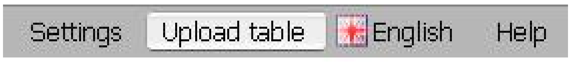
Deleting all users from the fingerprint Reader

- Right click on the Reader and select **Delete all**

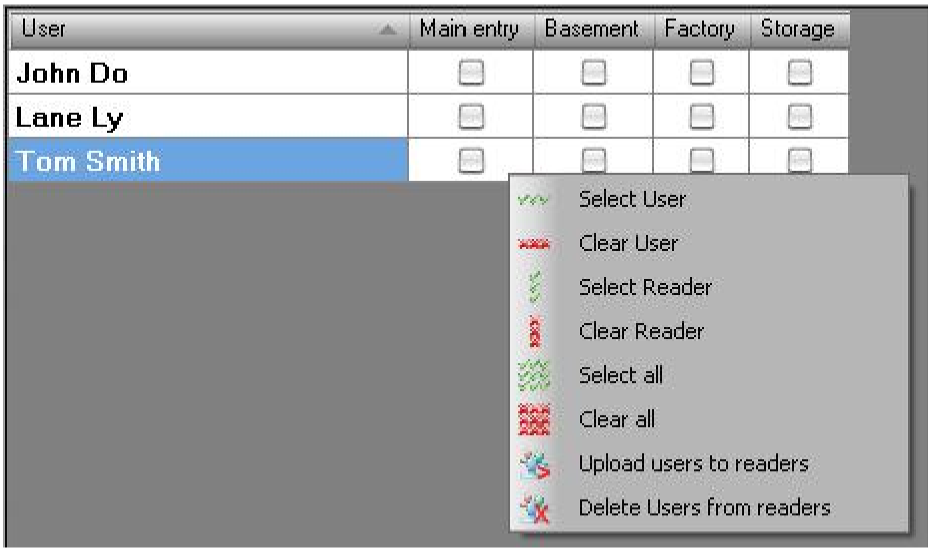
Complex user upload

Complex user upload is used to sent multiply user selection to more readers.

- Click on **Upload table** at main menu



- Use mouse click to select combination you need or use right-click to check or clear entire row or column



User	Main entry	Basement	Factory	Storage
John Do	□	□	□	□
Lane Ly	□	□	□	□
Tom Smith	□	□	□	□

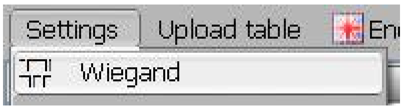
- Select **Upload Users to readers** or **Delete Users from readers** at right-click menu
- As upload is progressing, check boxes are cleared mining appropriate combination was successfully done
- When upload is over, if there is still checked items, repeat upload command

Custom Wiegand

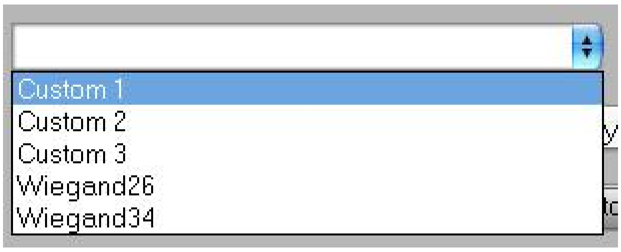
Biomanager have defined Wiegand 26 and 34 bit as standard options, and leave 3 wiegand settings as user definable.

To setup custom wiegand format

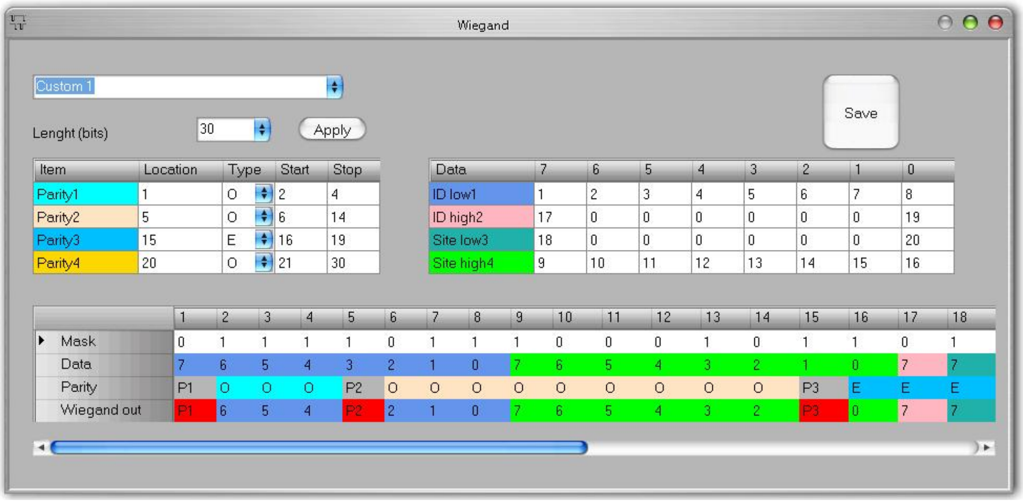
- Select **Wiegand** menu from **Settings**



- At wiegand setup window select one from customs wiegand



- Set wiegand parameters



Lenght (bits) 30

Item	Location	Type	Start	Stop
Parity1	1	O	2	4
Parity2	5	O	6	14
Parity3	15	E	16	19
Parity4	20	O	21	30

Data	7	6	5	4	3	2	1	0
ID low1	1	2	3	4	5	6	7	8
ID high2	17	0	0	0	0	0	0	19
Site low3	18	0	0	0	0	0	0	20
Site high4	9	10	11	12	13	14	15	16

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Mask	0	1	1	1	1	0	1	1	1	0	0	0	1	0	1	1	0	1
Data	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	7
Parity	P1	O	O	O	P2	O	O	O	O	O	O	O	O	O	P3	E	E	E
Wiegand out	P1	6	5	4	P2	2	1	0	7	6	5	4	3	2	P3	0	7	7

- Click on **Save** button

Note:

Wiegand settings are out of scope for common end user. Please ask your installer to set parameters and do not change if later.

Troubleshooting

- **Reader reading performance is decreased**

1. Check if fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use soft and dry cloth only.
2. Reading area is damaged. If damage is minor, try to calibrate the sensor

- **Fingerprint is not recognized normally**

1. Retry after drying the wetness of your finger
2. When your finger is too dry, touch your forehead and try again
3. When you have a cut on your registered finger, register another fingerprint.

- **Fingerprint is recognised but Control panel report other ID number**

1. If the user is not deleted from reader and user is enrolled again with new ID, reader will recognise finger with first ID. To resolve this, delete all users from reader and upload all users to reader

Glossary

A

Access Area: Space with restricted access by reader. One area can contain more separate areas. Can be one or group of rooms, parking lot, fence restricted area...
Access controller: When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a Control panel, a highly reliable processor. The control panel compares the credential's number to an internal access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a red LED for an access denied and a green LED for an access granted.Smart electronic with ability to remember User Id's, Time zones, Events, to control Doors, Relays, recieve informations of Door state, Inputs, Readers, Communicate with Access control software and to take action based on events and programmed parameters
Access level: Definition of time zones for each reader. Users can access readers only at time zones defined in Access level they belong. One user can be assigned only to one Access level. Same time zone can be used in unlimited number of Access levels.
Anti-passback: Prevention of allowing the user to enter area more than once with the same ID. It is prevention from borrowing the ID to another person in purpose of entering the area. This function is useful when higher level of security is needed, counting of persons in areas, time attendance, fire reports, etc. Anti-passback can have more variations. It can be valid for one or more readers, one or more doors, can be reset as fixed time of the day, can prevent double acces within a given period of time. Since Access controler is enforcing this restrictions, Anti-passback can be enforced only at doors and readers connected to the same controller.

B

Biometry: Way of recognising specific body parts specific to each person. Most common parts used in security systems are Fingerprint, Face, Eye, Finger vein, Voice and Palm. For higher security biometry can be mixed and combined with standard acces techniques like Fingerprint + Proximity card, Fingerprint + Code.

C

Code: Personal identification presented by typing a sequence of numbers to keypad. Depending on keypad model it can be fixed or variable length.
COM, COM port: Serial communication interface. Can be existing port in PC or can be external component. External component can be USB device with drivers of can be network device using drivers at PC side to create virtual COM port.
Control panel: Same as Access controller

D

Department: Grouping the users by internal organisation. Used for printing reports with convenient grouping of users.
Door contact sensor: The sensors are standard magnetic door sensors used in security applications. Either Normally Open or Normally Closed Sensors can be used. Recommended are Normally Closed sensors (door closed, switch closed) so that a alarm can be generated if the connection wire breaks.

E

Egress button, Exit switch: Push-button used to open the door from protected area side. Connected to Access controller. Electronic touch sensors can be used for same function.

Electric strike:access control device used for doors. It replaces the fixed strike faceplate often used with a latchbar (also known as a *keeper*). Like a fixed strike, it normally presents a ramped surface to the locking latch allowing the door to close and latch just like a fixed strike wouuld. However, an electric strike's ramped surface can, upon command, pivot out of the way of the latch allowing the door to be pushed open (from the outside) without the latch being retracted (that is, without any operation of the knob) or while exited the knob or lever can be turned to allow egress from the secured area.

Electric strikes generally come in two basic configurations:

- Fail-secure. Also called Fail-locked or non-fail safe. In this configuration, applying electrical current to the strike will cause it to open. In this configuration, the strike would remain locked in a power failure, but typically the knob can still be used to open the door from the inside for egress from the secure side. These units can be powered by AC which will cause the unit to "buzz", or DC power which will offer silent operation, except for a "click" while the unit releases.

- Fail-safe. Also called Fail-open. In this configuration, applying electrical current to the strike will cause it to lock. In this configuration, it operates the same as a magnetic lock would. If there is a power failure, the door would open merely by being pushed/pulled open. Fail safe units are always run using DC power.

F

Fingerprint reader: Reader with ability to recognise human finger and send information to Access controller.

Fire alarm input: Triggering this input will release all doors controlled by Control panel

Firmware: Programs and data structures that internally control various electronic devices

Free Input: Additional inputs available at Access controller. Not dedicated to primary role of Access control. Can be configured for additional monitoring of other events (Alarm, Fire..) or user action (Bell, Panic...)

Free output: Additional outputs available at Access controller. Not dedicated to primary role of Access control. Can be configured for execution of some tasks (Timer, Alarm bell, Light control..)

I

ID: Identification number presented to Access controler by Reader. Reader get information from media presented (Proximity card, Code, Biometry) and translate it to number format that Access controler can recognise.

Input: Hardware gate on Access controller able to recieve information about other equipement. It can be dedicated to specific task (door monitor, egress button..) or can be programmatically assigned to monitor other devices (Intruder alarm, fire, temperature). Access controller can be programmed to execute specific actions following the change of the inputs state. Inputs can have only two states (OFF/ON) . Inputs also are used to pass the information to Access control software.

IP Address: An **Internet Protocol** (**IP**) **address** is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes.

IP Port: A port number is a 16-bit unsigned integer, thus ranging from 0 to 65535. A process associates with a particular port (known as *binding*) to send and receive data, meaning that it will listen for incoming packets whose destination port number and IP destination address match that port, and/or send outgoing packets whose source port number is set to that port.

M

Magnetic lock: simple locking device that consists of an electromagnet and armature plate. By attaching the electromagnet to the door frame and the armature plate to the door, a current passing through the electromagnet attracts the armature plate holding the door shut.

Mantrap: Group of doors with logic that only one door can be open at the time. Opening the one of the door lock all other doors until it closes. Using combination of inputs and outputs mantrap can be extended to doors from different Access controllers in the same site.

O

Operator: Person listed at Access control software with given right to one or more options.

P

PIN Code: Personal identification presented by typing a sequence of numbers to keypad. Depending on keypad model it can be fixed or variable length.

Portal: Hardware interface between Access control software and devices installed in the system. One portal can connect one or more devices to software. Portal can be existing as single device or as a part of Access controller.

R

Reader: Device installed near access barrier (door, gate, turnstile..) to recognise user identification media (card, code, finger..) and send information to Access controller.

Relay: Electrical component used as output at Access controller. Provide eclectic isolation between Access controller and device that is controlled by output. Relay have two state: ON and OFF. Output of the relay provide mechanical switch contact with two outputs - one contact is open when relay is energised and other is closed.

.

T

Time zone: Definition of time period of the day used later to define system behaviour by time periods. Time zone also have definition of weekdays and holidays as additional filter for system behaviour.

Touch sensor: Electronic device reacting on human touch. Mostly used as egress button.

W

Wiegand interface: Wiring standard used to connect a card swipe mechanism to the rest of an electronic entry system. A Wiegand-compatible reader is normally connected to a Wiegand-compatible security panel.